IFW

TO: UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	Brian McKeon
Application/Control Number:	10/767,529
Original Filing Date:	29/Jan/2004
Art Unit:	2139
Examiner:	TABOR, AMARE F
For:	Regulated Issuance of Digital Certificates
Date:	11/Nov/2007

Dear Sir,
This document is filed in response to the Office Action dated 29/May/2008.

Thank you for the chance to respond to your review.

I hope that the attached discussion addresses your questions. If there are any of the above points that could be clarified via email or phone I can be contacted at brian.mckeon@sentrypm.com or on +61-413-401-555.

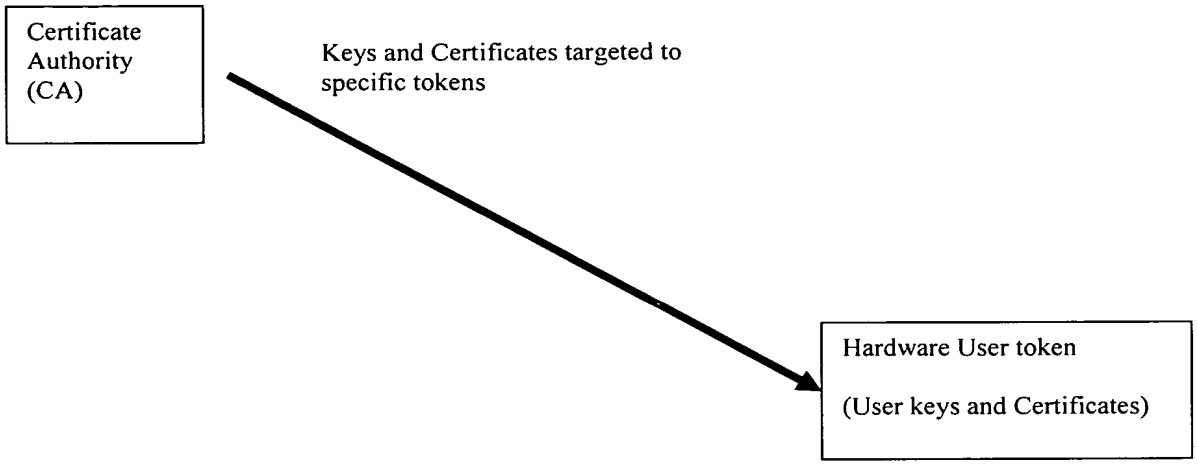
Yours Sincerely

Brian McKeon

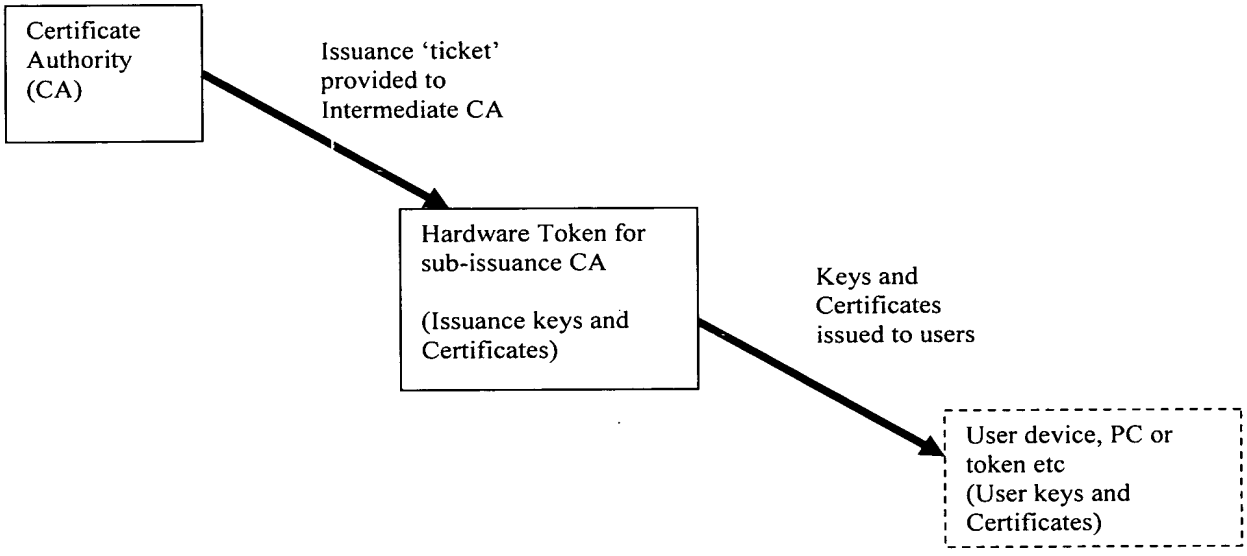
Brian McKeon

Attachments:
1. Discussion

The core claim of Aull shows that Aull is describing a system where each user has a hardware token that includes some credentials, those credentials allowing subsequent issuance of keys and certificates to be securely targeted at individual tokens. In essence the following figure shows the arrangement.



The invention disclosed in application 10/767,529 uses hardware tokens, not as a certificate and key store for end-users but as an intermediate Certificate Authority that can be securely regulated by the parent CA.



The intermediate, sub-issuance CA handles the routine requests from users for certificates. The main CA needs only deal with periodic requests for tickets, significantly lowering overheads on the main CA. The requirement for the hardware token at the sub-issuance CA is so that the main CA can be confident that

the certificates issued by the sub-issuance CA are regulated. That is, the number of certificates issued are regulated, and the format of the certificates is also regulated.

The hardware token for the sub-issuance CA also securely stores the sub-issuance keys of the CA. These are issuance keys that are for certification of user keys in the user tokens. Private user keys are not stored in the hardware token of the sub-issuance CA.

In application 10/767,529 we are not concerned with the hardware format of the end-user key and certificate storage. This is the reason why the text box surrounding the user credentials in the second figure is shown dashed. The user would use software key and certificate storage on a PC or may use a USB token, smartcard etc, depending on the security policy of their situation.